IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION

CHRISTOPHER MATESON
c/o Mason Lietz & Klinger LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016

Individually and on behalf of all others similarly situated,

Plaintiff,

v.

US FERTILITY, LLC
900 Blackwell Road, Suite 500
Rockville, MD 20850

s/o The Corporation Trust Inc.
2405 York Road, Suite 201
Lutherville, MD 21093

Defendant.

Case No. 8:21-cv-00466

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1. Negligence
2. Negligence *Per Se*
3. MD Consumer Protection Act
4. Unjust Enrichment

CLASS ACTION COMPLAINT

Plaintiff CHRISTOPHER MATESON ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant US FERTILITY, LLC ("USF" or "Defendant"), a Delaware domestic limited liability company, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record:

I. PARTIES

1. Plaintiff Christopher Mateson is, and at all times mentioned herein was, an individual citizen of the State of South Carolina residing in Summerville, South Carolina, and is a

patient of Coastal Fertility Specialists, an infertility clinic to which Defendant provides IT platforms and services. Plaintiff Mateson received notice of the data breach by letter dated January 8, 2021, and a copy of the notice is attached hereto as **Exhibit A**.

2. Defendant USF is a Delaware domestic limited liability company with its principal place of business in Rockville, Maryland.

II. JURISDICTION AND VENUE

5. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d). There are at least 100 Members in the Proposed Class, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000.00, exclusive of interest and costs, and Plaintiff and Members of the Proposed Class are citizens of states different from Defendant.

6. This Court has jurisdiction over Defendant, which operates and is headquartered in this District. The computer systems implicated in this Ransomware Attack/Data Breach are likely based in this District. Through its business operations in this District, USF intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

7. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District. Defendant is based in this District, maintains the personally identifiable information ("PII") and protected health information ("PHI") of Plaintiff and Class Members in this District, and has caused harm to Plaintiff and Class Members through its actions in this District.

III. NATURE OF THE ACTION

8. This class action arises out of the recent targeted malware infection, data breach, and ransomware attack against USF's network that encrypted data on a number of servers and workstations connected to USF's domain (the "Ransomware Attack" or "Data Breach"). The data affected included the PII and PHI of approximately 878,550 patients. In addition, the cyber criminals exfiltrated and stole data from USF's systems prior to the deployment of ransomware.

9. As a result of the Ransomware Attack, Plaintiff and Class Members suffered injury and damages. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to USF, its affiliates and agents—was compromised, unlawfully accessed, exfiltrated, and stolen from Defendant's systems prior to and during the Ransomware Attack. Information compromised in the Ransomware Attack includes names, addresses, dates of birth, MPI numbers, and Social Security numbers that Defendant collected (via its affiliates) and maintained (collectively the "Private Information").

10. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

11. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on USF's computer network in a condition vulnerable to phishing-initiated malware cyberattacks. As a result of the Ransomware Attack, Plaintiff's and Class Members' Private Information was encrypted and held hostage by computer hackers for "ransom," and also stolen (aka "exfiltrated"). Upon information and belief, the mechanism of the malware attack and subsequent ransomware deployment and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, as "phishing"

attacks are the "oldest trick in the book" in terms of cyberattacks. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

12. In addition, USF and its employees failed to properly monitor the computer network and systems that housed the Private Information, did not detect the initial intrusion into its systems that resulted in exfiltration of data, and ultimately only became aware that its systems had been compromised when the ransomware attack was unleashed. Had USF properly monitored its property, it would have discovered the intrusion sooner.

13. Because of the Ransomware Attack, Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct, as the Private Information that USF collected and maintained is now in the hands of data thieves.

14. Armed with the Private Information accessed and exfiltrated in the initial data breach and subsequent Ransomware Attack, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

15. As a further result of the Ransomware Attack, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

16. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. By his Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed, compromised, ransomed, or exfiltrated during the initial data intrusion and subsequent Ransomware Attack.

18. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

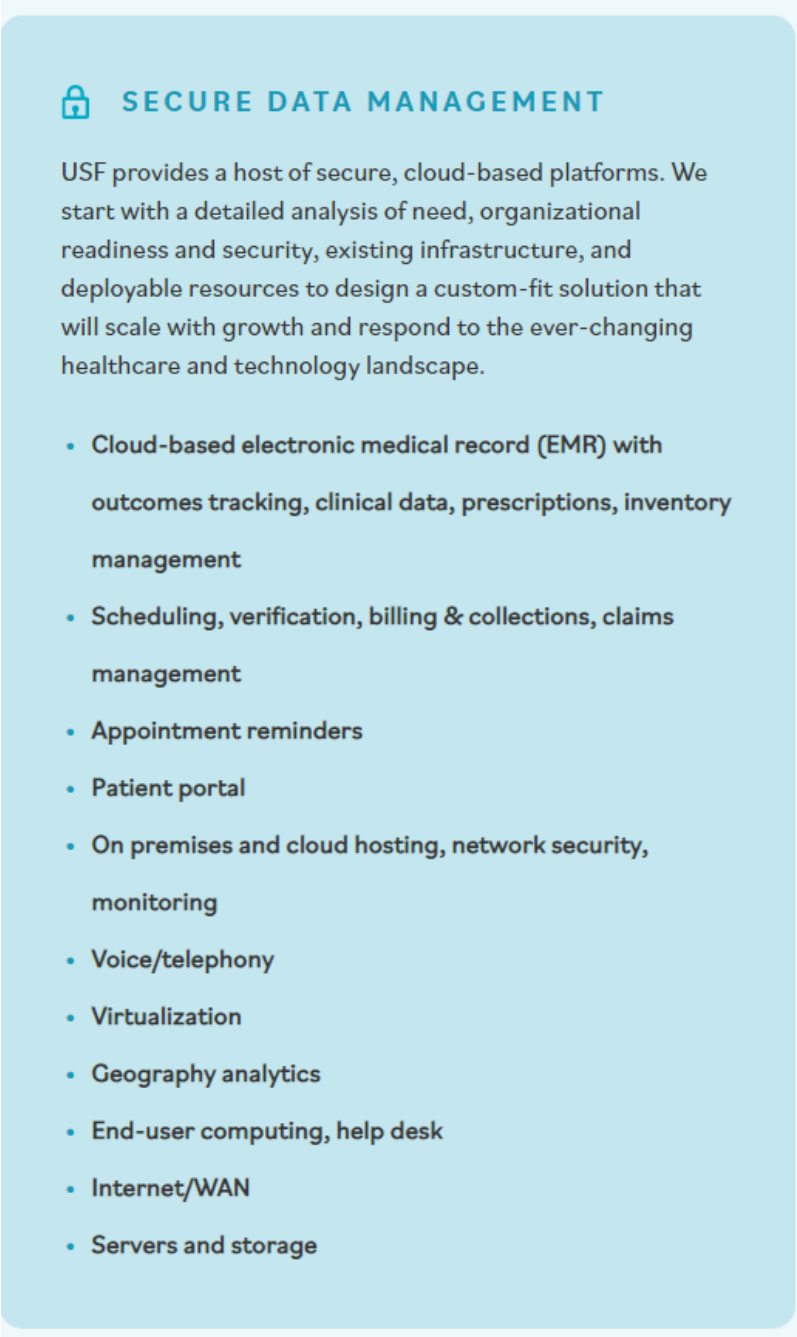
19. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence; (ii) negligence *per se*; (iii) unjust enrichment; and (iv) violation of the Maryland Consumer Protection Act.

DEFENDANT'S BUSINESS

21. According to its website, USF is "the largest network of fertility centers in the USA," and one of the largest support services networks for fertility clinics in the United States, providing administrative, clinical, and business information services.

22. USF touts its "advanced business and digital solutions" and access to "a variety of technical platforms" as part of the benefits to infertility clinics of partnering with USF.

23. As part of the Support Services it offers its partner and affiliate clinics, USF offers "Secure Data Management," which it describes as follows:



SECURE DATA MANAGEMENT

USF provides a host of secure, cloud-based platforms. We start with a detailed analysis of need, organizational readiness and security, existing infrastructure, and deployable resources to design a custom-fit solution that will scale with growth and respond to the ever-changing healthcare and technology landscape.

- Cloud-based electronic medical record (EMR) with outcomes tracking, clinical data, prescriptions, inventory management
- Scheduling, verification, billing & collections, claims management
- Appointment reminders
- Patient portal
- On premises and cloud hosting, network security, monitoring
- Voice/telephony
- Virtualization
- Geography analytics
- End-user computing, help desk
- Internet/WAN
- Servers and storage

24. In the ordinary course of receiving treatment and health care services from USF's affiliated and partner infertility clinics, all patients (including the named Plaintiff here) are required to provide Defendant (through its affiliate and partner clinics) with sensitive, personal and private information such as:

- Name, address, phone number and email address;

- Date of birth;
- Demographic information;
- Social Security number;
- Information relating to individual medical history;
- Insurance information and coverage;
- Information concerning an individual's doctor, nurse or other medical providers;
- Photo identification;
- Employer information; and
- Other information that may be deemed necessary to provide care.

25. USF's affiliate and partner clinics also gather certain medical information about patients and creates records of the care it provides to them.

26. Infertility is particularly sensitive and private and those going through treatments to have a baby have reasonable expectations that their PII and PHI will be protected and remain confidential.

THE DATA BREACH AND RANSOMWARE ATTACK

27. A ransomware attack is a cyberattack perpetrated with a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the victim pays a fee to the attacker.[1]

28. Ransomware attacks are often the final piece of a multiphase coordinated cyberattack. The computer systems of the cyberthieves' target are first infiltrated by malicious software commonly referred to as the "Initial Attack Vector," or "IAV." The IAV creates a means

[1] https://www.proofpoint.com/us/threat-reference/ransomware.

by which other malicious software, such as "Offensive Security Tools" or "OST," further infects the target's computer systems. The OST often contains the capability to exfiltrate data from the target's computer system, and to also erase all records of the malicious activity perpetrated. Once the cyberthieves have plundered the target's system using the IAV and OST, the cybercriminals unleash their ransomware virus, locking down the target's systems for a ransom.

29. On or about August 12, 2020, cyberthieves gained access to USF's computer network by way of a targeted "phishing" cyberattack.

30. Phishing attacks of the type launched against USF are among the oldest, most common, and well-known form of cyberattacks.

31. "Phishing is a cyber-attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need—a request from their bank, for instance, or a note from someone in their company—and to click a link or download an attachment."[2] The fake link will typically mimic a familiar website and require the input of credentials. Once inputted, the credentials are then used to gain unauthorized access into a system. "It's one of the oldest types of cyber-attacks, dating back to the 1990s" and one that every organization with an internet presence is aware."[3] It remains the "simplest kind of cyberattack and, at the same time, the most dangerous and effective."[4]

32. Phishing attacks are generally preventable with the implementation of a variety of proactive measures such as purchasing and using some sort of commonly available anti-malware

[2] Frulingher, J., "What is phishing? How this cyber-attack works and how to prevent it," CSO Online, Apr. 7, 2020 https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html (last visited June 20, 2020).
[3] *Id*.
[4] Phishing, Malwarebytes, https://www.malwarebytes.com/phishing/ (last visited June 20, 2020).

security software (such as the ubiquitous Malwarebites). Most cybersecurity tools have the ability to detect when a link or an attachment is not what it seems.[5]

33. Other proactive measures include sandboxing inbound e-mail (*i.e.*, an automated process that segregates e-mail with attachments and links to an isolated test environment, or a "sandbox," wherein a suspicious file or URL may be executed safely), inspecting and analyzing web traffic, penetration testing (which can be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incidents), and employee education, just to name some of the well-known tools and techniques to prevent phishing attacks.

34. Upon information and belief, the cyberattack that was launched from the inbox and email of at least one USF employee opened the door for malignant software (aka computer viruses, an IAV, OST, and a ransomware virus variant) to infect USF's computer networks.

35. USF was not aware that its systems were compromised, and between August 12, 2020 and September 14, 2020, the cyberthieves had unfettered access to Defendant's computer systems, and utilized that access to exfiltrate data from USF's systems.

36. The cyberattack and malicious software affected the security of patient data at the following infertility clinics associated with USF: Georgia Reproductive Specialists, LLC d/b/a SGF Atlanta, Center for Reproductive Endocrinology, Center for Reproductive Medicine & Advanced Reproductive Technologies, Center for Reproductive Medicine Alabama, Center for Reproductive Medicine Orlando, Coastal Fertility Specialists, Fertility Centers of Illinois, LLC, Fertility Partners of Pennsylvania Surgery Center, LLC, Idaho Center for Reproductive Medicine, Nevada Center for Reproductive Medicine, Nevada Fertility Center, New York Fertility Medical

[5] *Id.*

Practice, PLLC d/b/a SGF New York, Northwest Center for Infertility and Reproductive Endocrinology, LLP d/b/a IVF Florida Reproductive Associates, Reproductive Endocrinology Associates of Charlotte, Reproductive Partners Fertility Center - San Diego, Reproductive Partners Medical Group, Inc., Reproductive Science Center of the San Francisco Bay Area, Seattle Reproductive Medicine, SGF Tampa Bay, LLC, Shady Grove Fertility Center of Pennsylvania, PLLC, Shady Grove Reproductive Science Center, P.C., Sher Institute of Reproductive Medicine New York, Sher Institute of Reproductive Medicine St. Louis, UNC Fertility, Utah Fertility Center, Virginia Fertility Associates, LLC d/b/a SGF Richmond, and Virginia IVF and Andrology Center, LLC.

37. The data that was exfiltrated from USF's systems included names, addresses, dates of birth, MPI numbers, and Social Security numbers.

38. USF did not become aware that its computer systems were compromised and infected until the cyberthieves launched the Ransomware Attack on September 14, 2020.

39. The Ransomware Attack disrupted USF's computer network for six (6) days, from September 14, 2020 to September 20, 2020, leaving patient data stored on USF's network encrypted and inaccessible.

40. As a consequence of the cyber-attack on USF's computer systems, certain affected data was encrypted and locked away by the ransomware. This data included the Protected Health Information, or PHI, of patients of the infertility clinics affiliated with USF listed above, including Plaintiff and Class Members, who entrusted Defendant with this highly sensitive and private information.

41. On or about January 8, 2021, USF notified affected persons and various governmental agencies of the Ransomware Attack/Data Breach. The Notice of Data Incident ("Notice") sent to Plaintiff stated in relevant part the following:

> "On September 14, 2020, USF experienced an IT security event (the "Incident") that involved the inaccessibility of certain computer systems on our network as a result of a malware infection."
>
> "we determined that data on a number of servers and workstations connected to our domain had been encrypted by ransomware."
>
> "The forensic information is now concluded and confirmed that the unauthorized actor acquired a limited number of files during the period of unauthorized access, which occurred between August 12, 2020 and September 14, 2020, when the ransomware was executed."

See Exhibit A, Notice of Data Incident.

42. The Notice also informed Plaintiff that "the following information relating to you was included in the impacted files when they were accessed without authorization: name and SSN, Patient Number/MPI," and that the "impacted files may have also contained your date of birth." *Id.*

43. Based upon Defendant's admission in its Notice of Data Breach that patient data was exfiltrated, and that "impacted files" included Plaintiff's name, Social Security number, Patient Number/MPI, and possibly his date of birth, Plaintiff believes his Private Information was stolen (and subsequently sold) in the Ransomware Attack.

44. Plaintiff's belief that his Private Information was stolen is buttressed by a recent security advisory blog post from Microsoft that emphasized how healthcare ransomware attackers maintain their presence in breached computer systems (even systems that are rebuilt), and exfiltrate and steal data during these attacks:

> On networks where attackers deployed ransomware, they deliberately maintained their presence on some endpoints, intending to reinitiate malicious activity after ransom is paid or systems are rebuilt. In addition, while only a few of these groups gained notoriety for

selling data, almost all of them were observed viewing and exfiltrating data during these attacks, even if they have not advertised or sold yet.[6]

45. Despite learning of the ransomware attack on September 14, 2020, USF did not begin providing notice of the data breach to its patients until November 25, 2020, and did not notify Plaintiff until January 8, 2021.

DEFENDANT'S LEGAL DUTIES

46. Defendant had obligations created by HIPAA, contract, industry standards, and common law to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

47. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

FORESEEABILITY OF THIS CYBERATTACK

48. Defendant's data security obligations were particularly important given the substantial increase in ransomware attacks and/or data breaches in the healthcare industry preceding the date of the breach, and this ransomware attack was completely foreseeable to Defendant and any entity in the healthcare industry.

49. Data breaches, including those perpetrated against the healthcare sector of the economy, have become widespread. In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year. In 2017, a new record high of 1,579 breaches were reported, representing a 44.7 percent increase over 2016. In 2018, there was an extreme jump of 126 percent in the number of consumer records

[6] https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

exposed from data breaches. In 2019, there was a 17 percent increase in the number of breaches (1,473) over 2018, with 164,683,455 sensitive records exposed.

50. The number of data breaches in the healthcare sector skyrocketed in 2019, with 525 reported breaches exposing nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.

51. Indeed, ransomware attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[7]

52. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and reasonably foreseeable to the public and to anyone in Defendant's industry, including Defendant USF.

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

53. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

54. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that

[7] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (emphasis added).

businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

55. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

56. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In re Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

58. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

59. Defendant was at all times fully aware of its obligation to protect the PII and PHI of the patients of its affiliate clinics. Defendant was also aware of the significant repercussions that would result from its failure to do so.

DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

60. As shown above, experts studying cyber security routinely identify healthcare providers (and companies like USF that service healthcare providers) as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

61. As an article about the recent Microsoft study stated, "All hospitals and healthcare organizations need to defend themselves against ransomware, especially during this challenging time."[8] Microsoft provided a list of 11 best practices tips for how hospitals should protect themselves against ransomware.

62. Several best practices have been identified that a minimum should be implemented by entities like Defendant that service healthcare providers, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

[8] https://www.techrepublic.com/article/microsoft-to-hospitals-11-tips-on-how-to-combat-ransomware/

63. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security ("CIS") released its Critical Security Controls, and all healthcare institutions are strongly advised to follow these actions. The CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[9]

64. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

65. Defendant failed to meet the minimum standards of any of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

66. These foregoing frameworks are existing and applicable industry standards in Defendant's industry.

[9] https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/

DEFENDANT'S CONDUCT VIOLATES HIPAA AND EVIDENCES ITS INSUFFICIENT DATA SECURITY

67. Defendant USF is a "covered entity" under HIPAA.

68. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

69. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

70. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

71. Defendant's Ransomware Attack/Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT'S BREACH

72. The Data Breach and Ransomware Attack were the result of USF's inadequate and lax approach to cybersecurity and the protection of its customers' PII that it collected in the normal course of its business.

73. Upon information and belief, prior to the cyberattack USF had in place an inadequate or non-updated firewall and had not properly trained its employees to recognize phishing emails.

74. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords;

i. Failing to properly train and supervise employees in the proper handling of inbound emails;

j. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

k. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

l. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

m. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

n. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

o. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

p. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

q. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its

workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

r. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

75. USF could have prevented the Data Breach from occurring. USF failed to take adequate and reasonable measures to ensure its computer/server systems were protected against unauthorized access and failed to take actions that could have stopped the Data Breach before it occurred.

76. USF failed to disclose to Plaintiff and Class Members that its computer/server systems and security practices were inadequate to reasonably safeguard their PII and failed to immediately notify them of the data theft.

77. As the result of computer systems in dire need of cybersecurity upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant USF negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

78. Accordingly, as outlined below, Plaintiff and Class Members now face an imminent risk of fraud and identity theft.

RANSOMWARE ATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

79. Ransomware attacks against companies like USF that support medical providers are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

80. For instance, loss of access to patient histories, charts, images and other information forces providers to limit or cancel patient treatment because of the disruption of service.

81. This leads to a deterioration in the quality of overall care patients receive at facilities affected by ransomware attacks and related data breaches.

82. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[10]

83. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in patient outcomes, generally.[11]

84. Similarly, ransomware attacks and related data security incidents inconvenience patients. Inconveniences patients encounter as a result of such incidents include, but are not limited to, the following:

a. rescheduling medical treatment;

b. finding alternative medical care and treatment;

c. delaying or foregoing medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

[10] *See* https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.
[11] *See* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

e. losing patient medical history.[12]

85. Ransomware attacks such as this one, where USF confirms that data was exfiltrated, also constitute data breaches in the traditional sense.

86. Also, in a ransomware advisory, the Department of Health and Human Services informed entities covered by HIPAA that "when electronic protected health information ("ePHI") is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (*i.e.*, unauthorized individuals have taken possession or control of the information)."[13]

87. Ransomware attacks are also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, " . . . the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40[14]

88. Other security experts agree that when ransomware attack occurs, a data breach does as well, because such an attack represents a loss of control of the data within a network.[15]

89. Ransomware attacks are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule.

---

[12] *See, e.g.*, https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/;https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech.

[13] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

[14] *Id.*

[15] *See e.g.*, https://www.csoonline.com/article/3385520/how-hackers-use-ransomware-to-hide-data-breaches-and-other-attacks.html; https://www.varonis.com/blog/is-a-ransomware-attack-a-data-breac h/; https://digitalguardian.com/blog/ransomware-infection-always-data-breach-yes.

> A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. *See* the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. *See* 45 C.F.R.164.308(a)(6).[16]

90. Data breaches represent yet another problem for patients whose data was compromised in a ransomware attack.

91. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[17]

92. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[18]

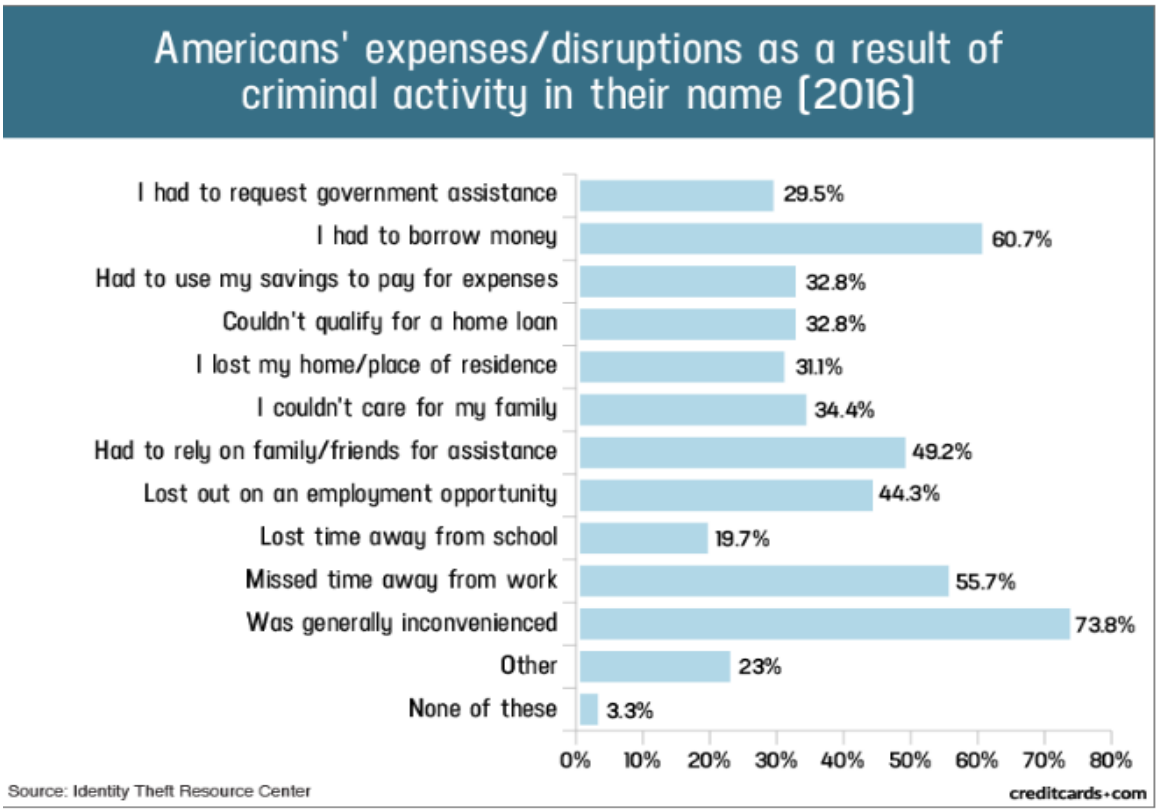
93. Identity thieves use stolen personal information such as Social Security numbers to commit a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

94. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name

---

[16] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
[17] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Gov't Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").
[18] *See* https://www.identitytheft.gov/Steps (last visited Apr. 12, 2019).

and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[19]



95. What's more, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[20] Its value is axiomatic, considering the value of Big Data in corporate

[19] Jason Steele, "Credit Card and ID Theft Statistics" (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited June 20, 2019).

[20] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3–4

America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

96. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[21] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

97. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report at 29.

(2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[21] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Mar. 27, 2020).

98. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" or "dark web" for years.

99. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

100. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[22]

101. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[23]

102. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016—the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $50 and up.[24]

---

[22] A. George, "Your personal data is for sale on the dark web. Here's how much it costs," Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Feb. 19, 2021).

[23] Social Security Administration, Identity Theft and Your Social Security Number, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Feb. 19, 2021).

[24] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crus h-hospitals/#content.

103. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFF'S AND CLASS MEMBERS' INJURY AND DAMAGES

104. To date, Defendant has done absolutely nothing beyond offering an inadequate 12 months of credit monitoring to provide Plaintiff and certain (but not all) Class Members with relief for the damages they have suffered as a result of the Ransomware Attack. Nor has Defendant offered any protection against the imminent, likely, and probable effects that will result from Plaintiff's and Class Members' Private Information being stolen in connection with the attack.

105. Plaintiff and Class Members have been injured and damaged by the access to, compromise of, exfiltration of, and theft of their Private Information in the Ransomware Attack.

106. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

107. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

108. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

109. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Ransomware Attack.

110. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Ransomware Attack. Numerous courts have recognized the propriety of loss of value damages in related cases.

111. Class Members were also damaged via benefit-of-the-bargain damages, in that they overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of USF's computer property and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for.

112. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

113. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Ransomware Attack. In addition to the loss of use of and access to their medical records and costs associated with the inability to access their medical records, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Ransomware Attack relating to:

a. Finding alternative medical care and treatment;

b. Delaying or foregoing medical care and treatment;

c. Undergoing medical care and treatment without medical providers having access to a complete medical history and records;

d. Having to retrace or recreate their medical history;

e. Finding fraudulent charges;

f. Canceling and reissuing credit and debit cards;

g. Purchasing credit monitoring and identity theft prevention;

h. Addressing their inability to withdraw funds linked to compromised accounts;

i. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

j. Placing "freezes" and "alerts" with credit reporting agencies;

k. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

l. Contacting financial institutions and closing or modifying financial accounts;

m. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

n. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

o. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

114. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

115. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains some of the most intimate details about a person's life (fertility issues)—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

116. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

IV. CLASS ACTION ALLEGATIONS

117. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class").

118. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> The Class
>
> All persons whose PII and PHI was compromised as a result of the Ransomware Attack that USF discovered on or about September 14, 2020, and who were sent notice of the data breach by USF.

Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

119. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The Proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

120. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of 878,550 patients of Defendant USF whose data was compromised in the Ransomware Attack.

121. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Ransomware Attack;

c) Whether Defendant's data security systems prior to and during the Ransomware Attack complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

d) Whether Defendant's data security systems prior to and during the Ransomware Attack were consistent with industry standards;

e) Whether Defendant owed a duty to Plaintiff and Class Members to safeguard their Private Information;

f) Whether Defendant breached its duty to Plaintiff and Class Members to safeguard their Private Information;

g) Whether computer hackers obtained Class Members' Private Information in the Ransomware attack;

h) Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j) Whether Defendant owed a duty to provide Plaintiff and Class Members notice of this data breach, and whether Defendant breached that duty;

k) Whether Defendant's conduct was negligent;

l) Whether Defendant's conduct was *per se* negligent;

m) Whether Defendant was unjustly enriched;

n) Whether Defendant violated the Maryland Consumer Protection Act; and

o) Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

122. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Ransomware Attack.

123. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

124. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer network and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any

individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

125. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

126. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

127. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII and PHI;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII and PHI; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

128. Finally, all Members of the Proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant USF.

V. CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiff and All Class Members)

129. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 128 above as if fully set forth herein.

130. Defendant required Plaintiff and Class Members to submit non-public personal information in order to obtain medical services.

131. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's

duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

132. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

133. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

134. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

135. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

136. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

137. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Ransomware Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

138. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

139. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Plaintiff and Class Members.

140. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Ransomware Attack.

141. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Negligence *Per Se*
(On Behalf of Plaintiff and All Class Members)

142. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 128 above as if fully set forth herein.

143. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

144. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

145. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

146. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et seq.*, Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

147. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA

Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

148. Plaintiff and Class Members are within the class of persons that the HIPAA was intended to protect.

149. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiff and the Class.

150. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

151. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

152. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

153. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

154. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

THIRD COUNT
Violation of the Maryland Consumer Protection Act
(On Behalf of Plaintiff and the Class)

155. Plaintiff restates and realleges paragraphs 1 through 128 as if fully set forth herein.

156. This cause of action is brought pursuant to the Maryland Consumer Protection Act, § 13-101, *et seq*.

157. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices in the State of Maryland by:

a. failing to maintain adequate computer systems and data security practices to safeguard PHI;

b. failing to disclose that its computer systems and data security practices were inadequate to safeguard PHI from theft; and

c. continued gathering and storage of PHI and other personal information after Defendant knew or should have known of the security vulnerabilities of its computer systems that were exploited in the Ransomware Attack.

158. These unfair acts and practices violated duties imposed by laws, including but not limited to Section 5 of the Federal Trade Commission Act, and HIPAA.

159. USF is a "person" within the meaning of MD Comm. L. Code § 13-101(h) (2019).

160. Plaintiff and Class Members are "consumers" within the meaning of MD Comm. L. Code § 13-101(c)(1), in that they actual purchasers of USF's consumer services.

161. USF has committed an unfair, abusive or deceptive trade practice as that term is defined in MD Comm. L. Code § 13-301. The provisions violated by Defendant include, but are not limited to, the following:

a. Section 13-301(3) – failure to state a material fact (the inadequacy of USF's cyber and data security) if the failure deceives or tends to deceive; and

b. Section 13-301(9) – knowing concealment, suppression, or omission of a material fact with the intent that a consumer rely on the same in connection with the promotion or sale of a consumer service.

162. The acts and omissions of USF were done knowingly and intentionally with the purpose of the sale of consumer services to the Plaintiff and Class Members.

163. Plaintiff and Class Members were injured because they would not have purchased consumer services from USF had they known the true nature and character of Defendant's data security practices.

164. Defendant has violated the Maryland Consumer Protection Act by engaging in the unfair, abusive, and deceptive practices alleged herein. Pursuant to HIPAA (42 U.S.C. § 1302d, *et seq.*), the FTCA, and Maryland law, Defendant was required by law, but failed, to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Private Information. This constitutes a violation of Maryland's Consumer Protection Act.

165. The damages suffered by Plaintiff and Class Members were directly and proximately caused by the deceptive, abusive, and unfair practices of Defendant, as described above.

166. Plaintiff and Class Members seek declaratory judgment that Defendant's data security practices were not reasonable or adequate and caused the Ransomware Attack under the Maryland CPA, as well as injunctive relief enjoining the above described wrongful acts and practices of Defendant USF and requiring Defendant USF to employ and maintain industry accepted standards for data management and security, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

167. Additionally, Plaintiff and Class Members make claims for actual damages, attorneys' fees and costs.

FOURTH COUNT
Unjust Enrichment
(On Behalf of Plaintiff and All Class Members)

168. Plaintiff restates and realleges paragraphs 1 through 128 above as if fully set forth herein.

169. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

170. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

171. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Ransomware Attack,

Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

172. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

173. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

174. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

175. Plaintiff and Class Members have no adequate remedy at law.

176. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate

measures to protect PII and PHI in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

177. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

178. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Ransomware Attack;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h) Pre- and post-judgment interest on any amounts awarded; and

i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: February 23, 2021

Respectfully submitted,

Gary E. Mason (MD Fed. Bar No. 15033)
David K. Lietz*
MASON LIETZ & KLINGER LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Tel: (202) 429-2290
Fax: (202) 429-2294
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (202) 975-0477
Fax: (202) 429-2294
gklinger@masonllp.com

**pro hac vice to be filed*

Attorneys for Plaintiff and the Proposed Class